(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization

International Bureau





(43) International Publication Date 2 December 2004 (02.12.2004)

PCT

(10) International Publication Number WO 2004/105306 A1

(51) International Patent Classification7:

H04L 9/06

(21) International Application Number:

PCT/IB2004/001690

(22) International Filing Date:

19 May 2004 (19.05.2004)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

60/473,209

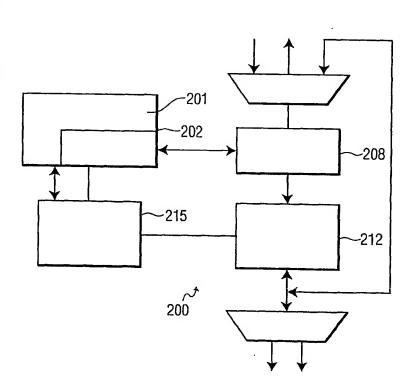
23 May 2003 (23.05.2003) US

- (71) Applicant (for all designated States except US): KONIN-KLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): SEXTON, Bonnie, C. [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

- (74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; c/o Waxler, Aaron, P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR A LOW MEMORY HARDWARE IMPLEMENTATION OF THE KEY EXPAN-SION FUNCTION



(57) Abstract: An apparatus, method and computer program for reducing memory space required during the key expansion function in algorithms such as AES. A block round unit (212) for encrypting/decrypting the predetermined number of byte units into ciphered text/plain text. A key expansion module (215) performs key expansion on both normal (encryption) and inverse (decryption) functions to obtain expanded key values. The number of memory spaces in the memory (202) required for storage of the expanded key values is no greater than half the number of expanded key values and typically requires 7 memory spaces for 14 keys without an increase in access time relative to a case when the number of key values and memory spaces are equal. The key expansion is perform in synchronization with Round Key processing so that for each key expansion a Round Key is being processed in parallel with a respective key expansion function.

WO 2004/105306 A1

WO 2004/105306 A1



Declarations under Rule 4.17:

as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

- IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.